ETHICAL HACKING

***Selvanayki.S**

***Sumathi.P**

***Soundariya.S.S**

ABSTRACT

Ethical hacking is also called as penetration testing,intrustion testing or red teaming. Ethical hacking is one of the controversial act of locating weakness and vulnerabilities of computer and information system but duplicating the intent and actions of malicious hackers. An ethical hacker also known as a whitehat hacker or simply called as whitehat. It is security professional who applies their hacking skills for defensive purposes of information systems. The certified ethical hackers are the most sought after information security employees in the large organisations such as wipro, infosys, ibm, airtel and reliance among others.

1. INTRODUCTION

Ethical hacking refers to the act of locating weaknessses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing, or redteaming. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. By conducting penetration tests, an ethical hacker looks to answer the four basic questions;

1.What information/locations/systems can an attacker gain access?

2.What can an attacker see on the target?

3.What can an attacker do with available information?

4.Does anyone at the target system notice the attempts?

An ethical hacker operates with the knowledge and permission of the organization for which they are trying to defend. In some cases, the organization will neglect to inform their information security team of the activities that will be carried out by an ethical hacker in an attempt to test the effectiveness of the information security team. This is referred to as a double-blind environment. In order to operate effectively and legally, an ethical hacker must be informed of the assets that should be protected , potential threat sources, and the extent to which the organization will support an ethical hacker's efforts.

1.1. ETHICAL HACKING HISTORY

Since the 1980's, the internet has vastly grown in popularity and computer security has become a major concern for business and governments. Organization would like to use the internet to their advantage by utilizing the internet as a medium for e-commerce, advertising, information distripution and access, as well as other endeavors. However, they remain worried that they may be hacked which could lead to a loss of control of private and personal information regarding the organisation, its employees, and its client.

In a search for way to reduce the fear and worry of being hacked, organizations have come to the realization that an effective way to evaluate security threats is to have independent security exerts attempt to hack into their computer systems. In the case of computer security, these tiger teams or ethical hackers would use the same tools and techniques as an attacker, but rather than damage the system or steal information, they would evaluate the system security and report the vulnerabilities they found and provide instructions for how to remedy them.

From the early days of computers, ethical hacking has been used as an evaluation of system security. Many early ethical hacks were conducted by the united states military to cary out security evaluations on their operating systems to determine whether they should employ a two-level (secret/top secret) classification system. However, With the growth of computing and networking in the early 1990's, computer and network vulnerability studies began to appear outside of the military organization. In december of 1993, two computer security researchers, dan farmer from elemental security and wietse venema from IBM suggested that the security of an information system. They wrote a report that was shared publicly on the internet which described how they were able to gather enough information to compromise security and they provided several examples of how this information could be gathered and exploited to gain control of a system, and how such an attack could be prevented.

Farmer and venema realized that the testing that they had performed was complex and time-consuming, so they packaged all of the tools that they had used during their work and developed an easy-to-use application free foe download. Their program, called security analysis tool for auditing networks, or satan, received a great amount of media attention due to its capability as well as capabilities to provide advice regarding how the user may be able to correct the problems that were discovered.

2. THE ETHICAL HACKING PROCESS

Ethical hacker must follow a strict scientific process in order to obtain useable and legal results.

2.1. PLANNING

- Planning is essential for successful project. It provides an opportunity to give critical thought to what needs to be done, allows for goals to be set, and allows for a risk assessment to evaluate how a project should be carried out.

- There are a large number of external factors that need to be considered when planning to carry out an ethical hack. These factors include existing security policies, culture, laws and regulations, best practices, and industry requirements. Each of these factores play an integral role in the decision making process when it comes to ethical hacking. The planning phase of an ethical hack will have a profound influence on how the hack is performed and the information shared and collected, and will directly influence the deliverable and integration of the results into the security program.

- The planning phase will describe many of the details of a controlled attack. It will attempt to answer questions regarding how the attack is going to be supported and controlled, what the underlying actions that must be performed and who does what, where, and for how long.

2.2. RECONNAISSANCE

- Reconnaissance is the search for freely available information to assist in an attack. This can be as simple a ping or browsing newsgroups on the internet in search of disgruntled employees divulging secret information or as messy as digging through the trash to find receipts or letters.

- Reconnaissance can include social engineering, tapping phones and networks, or even theft. The search for information is limited only by the extremes at which the organization and ethical hacker are willing

to go in order to recover the information they are searching for.

- The reconnaissance phase introduces the relationship between the task that must be completed and the methods that will need to be used in order to protect the organization assets and information.

2.3. ENUMERATION

- Enumeration is also known as network or vulnerability discovery. It is the act of obtaining information that is readily available from the target system,applications and networks. It is important to note that the enumeration phase is often the point where the line between an ethical hack and a malicious attack can become blurred as it is often easy to go outside of the boundaries outlined in the original attack plan.

- In order to construct a picture of an organization environment, several tools and techinques are available. These tools and techinques include port scanning and nmap. Although it is rather simple to collect information, it is rather difficult to determine the value of the information in the hands of a hacker.

- At first glance, enumeration is simple take the collected data and evaluate it collectively to establish plan for more reconnaissance or building a matrix for the vulnerability analysis phase. However, the enumeration phase is where the ethical hacker's ability to make logical deductions plays an enormous role.

2.4. VULNERABILITY ANALYSIS

- In order to effectively analyze data, an ethical hacker must employ a logical and pragmatic approach. In the vulnerability analysis phase, the collected information is compared with known vulnerabilities in a practical process.

- Information is useful no matter what the source. Any little bit can help in discovering options for exploitation and may possibly lead to discoveries that may not have been found otherwise. Known vulnerabilities, incidents, service packs, updates, and even available hacker tools help in identifying a point of attack. The Internet provides a vast amount of information that can easily be associated with the architecture and strong and weak points of a system.

2.5. EXPLOITATION

- A significant amount of time is spent planning and evaluated an ethical hack. Of course, all this planning must eventually lead to some form of attack. The exploitation of a system can be as easy as running a small tool or as intricate as a series of complex steps that must be executed in a particular way in order to gain access.

- The exploitation process is broken down into a set of subtasks which can be many steps or a single step in performing the attack. As each step is performed, an evaluation takes place to ensure that the expected outcome is being met. Any divergence from the attack plan is classified into two determinations:

- Expectations: Are the expectations of the exploitation being met or are the results conflicting with the organization's assumptions?

- Technical: Is the system reacting in an unexpected manner, which is having an impact on the exploitation and the engagement as a whole?

2.6. FINAL ANALYSIS

- Although the exploitation phase has a number of checks and validations to ensure success, a final analysis is required to categorize the vulnerabilities of the system in terms of their level of exposure and to assist in the derivation of a mitigation plan. The final analysis phase provides a link between the

exploitation phase and the creation of a deliverable.

- A comprehensive view of the entire attack must exist in order to construct a bigger picture of the security posture of the environment and express the vulnerabilities in a clear and useful manner. The final analysis is part interpretation and part empirical results.

2.7. DELIVERABLES

- Deliverables communicate the results of tests in numerous ways. Some deliverables are short and concise, only providing a list of vulnerabilities and how to fix them, while others are long and detailed, providing a list of vulnerabilities with detailed descriptions regarding how they were found, how to exploit them, the implications of having such a vulnerability and how to remedy the situation.
- The deliverable phase is a way for an ethical hacker to convey the results of their tests. Recently, ethical hacking has become so commoditized that if a deliverable does not instill fear into the hearts of executives, it could be considered a failure.

2.8. INTEGRATION

- Finally, it essential that there is some means of using the test results for something productive. Often, the deliverable is combined with existing materials, such as a risk analysis, security policy, previous test results, and information associated with a security program to enhance mitigation and develop remedies and patches for vulnerabilities.
- There are three distinguishing factors that should be considered during the integration of any test results:
- Mitigation: If vulnerability beyond acceptable risk was found, then it would need to be fixed. Mitigation of a vulnerability can include testing, piloting, implementing, and validating changes to systems.
- Defense: Vulnerabilities need to be addressed in a strategic manner in order to minimize future or undetected vulnerabilities. Defense planning is establishing a foundation of security to grow on and ensure long-term success.
- Incident Management: The ability to detect, respond, and recover from an attack is essential. Knowing how attacks are made and the potential impacts on the system aids in formulating an incident response plan. The ethical hacking process provides an opportunity for discovering the various weaknesses and attractive avenues of attack of a system which can aid in preventing future attacks.

3. 10 COMMANDMENTS OF ETHICAL HACKING

Becoming a believer in the doctrine of ethical hacking, requires that one following the 10 Commandments of Ethical Hacking [5] described below:

1.Thou shalt set thy goals

An ethical hacker should set simple goals, such as finding unauthorized wireless access points or obtaining information from a wired network system. In any case, the goals should be articulate and well communicated.

2. Thou shalt plan thy work, lest thou go off course

Ethical hackers are bound by constraints. Consequently, it is important to develop a strategy plan which should include identifying the networks to test, specifying the testing interval, specifying the testing process, and obtaining approval of the plan.

3. Thou shalt obtain permission

Written permission is required and should state that an ethical hacker is authorized to perform a test according to the plan. It should also say that the organization will provide legal and organizational support in case criminally charges or lawsuits arise. This is conditional on staying within the bounds of the approved plan.

4. Thou shalt work ethically

An ethical hacker is bound to confidentiality and non-disclosure of information they may uncover. Ethical hackers must also be compliant with their organization's governance and local laws. An ethical hack must not be performed when the company policy or the law for that matter, explicitly forbids it.

5. Thou shalt keep records

Patience and thoroughness are attributes of a good ethical hacker. A hallmark of ethical hacker professionalism is keeping adequate records to support findings. The date and details regarding each test, whether or not they were successful, should be logged and recorded and a duplicate copy of the log book should be kept.

6. Thou shalt respect the privacy of others

An ethical hacker must not abuse their authority. Ethical hackers must snoop into confidential corporate records or private lives. The information that is uncovered should be treated with the same care one would give to their own personal information.

7. Thou shalt do no harm

The actions of an ethical hacker may have unplanned repercussions. It is easy to get caught up in the work and cause a denial of service or trample on someone else's rights. It is important to stick to the original plan.

8. Thou shalt use a scientific process

The work of an ethical hacker should adopt an empirical method. An empirical method will help set quantifiable goals, develop consistent and repeatable tests, and provide tests that are valid in the future.

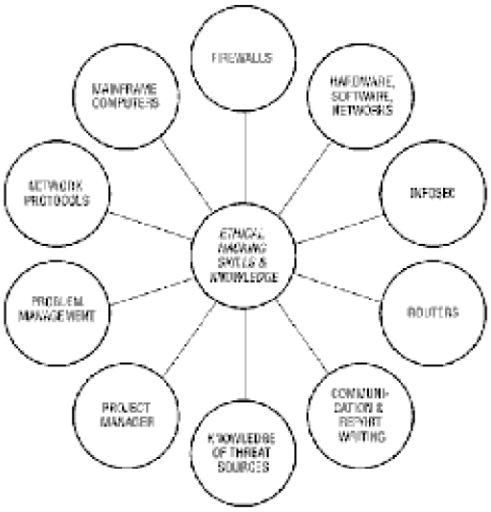
9. Thou shalt not covet thy neighbour's tools

Ethical hackers will always discover new tools to help them get their job done. Tools are abundant on the Internet and more are coming out all the time. The temptation to grab them all is fierce. Although it is possible to use all of the tools that are available, it is recommended that an ethical hacker choose one and stick with it.

10. Thou shalt report all thy findings

Ethical hackers should plan to report any high-risk vulnerabilities discovered during testing as soon as they are found. Reports are one way for the organization to determine the completeness and thoroughness of the work of an ethical hacker and provides a means for peers to review methodologies, findings, analysis, and conclusions.

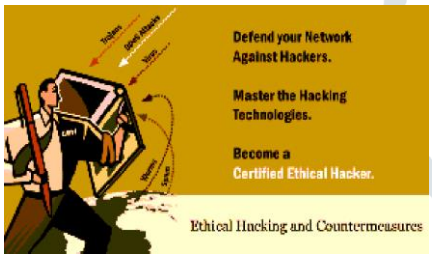
4. REQUIRED SKILLS



Required skills of an ethical hackers

- An ethical hacker is required to possess a vast arrangement of computer skills. It is not feasible for each ethical hacker to be an expert is every field and thus ethical hacking tiger teams whose members have complementing skills are created to provide an organization with a team possessing the complete skill set required of an ethical hacker.
- Organizations may have a wide variety of computer systems and it is essential for any ethical hacker to have expertise in operating systems, as well as network hardware platforms. It is also fundamental that an ethical hacker posses a solid foundation of the principles of information security .

5. CERTIFICATION



Certified Ethical Hacker Poster

- Due to the controversy surrounding the profession of ethical hacking, the International Council of E-Commerce Consultants (EC-Council) provides a professional certification for Certified Ethical Hackers (CEH). A certified ethical hacker is an ethical hacker who has obtained the certification provided by the EC-Council. As of August 2008, the certification is in Version 6.
- In order to obtain certification, an ethical hacker must complete a coursework consisting of 22 modules, which range from 30 minutes to 5 hours or more, depending on the depth of the information provided. The modules are as follows [6]:

1. Legality 2. Footprinting 3. Scanning 4. Enumeration 5. System Hacking 6. Trojans & Backdoors 7. Sniffers 8. Denial of Service 9. Social Engineering 10. Session Hacking 11. Hacking Web Servers 12. Web Application Vulnerabilities 13. Web-based Password Cracking 14. SQL Injection 15. Hacking Wireless Networks 16. Viruses 17. Physical Security 18. Linux Hacking 19. Evading Intrusion Detection Systems 20. Buffer Overflows 21. Cryptography 22. Pen Test Methodologies

- After having attended all coursework modules, an ethical hacker must write an exam (CEH Exam 312-50) consisting 150 multiple-choice questions in 4 hours. A score of 70% is required to pass the examination. A sample question from the CEH Exam 312-50 is as follows [7]:

- This tool is a a file and directory integrity checker. It aids system administrators in monitoring a designated set of files for any changes.

A. NMap

B. Integricheck

C. DSniff

D. Cybercop Scanner

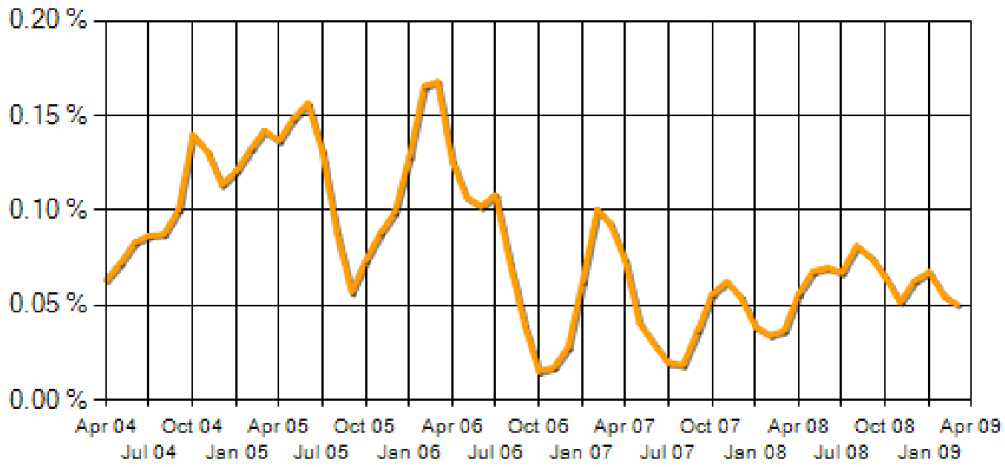
E. Tripwire

The examination fee is US$250 and is administered via computer at an EC-Council Accredited Training Center. Upon completion of the certification, ethical hackers holding the CEH designation will be required to re-certify under this program every three years.

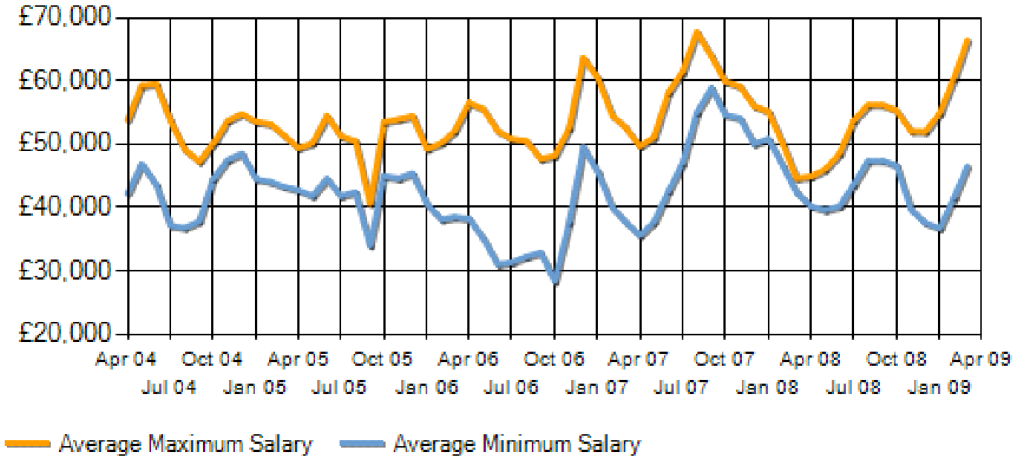
6. SALARIES AND TRENDS

A survey done by the International Data Corp (IDC) says that the worldwide demand for information security professionals stands at 60,000 and companies such as Wipro, Infosys, IBM, Airtel and Reliance are always looking for good ethical hackers.

In the United Kingdom, the following trends have been seen for demand and salaries of ethical hackers.



The above chart provides the 3-month moving total beginning in 2004 of permanent IT jobs citing Ethical Hacking within the UK as a proportion of the total demand within the Processes & Methodologies category [8].



The above chart provides the 3-month moving average for salaries beginning in 2004 of permanent IT jobs citing Ethical Hacking within the UK [8].

The average salary for an ethical hacker in the United Kingdom is approximately 56,000 pounds which is approximately CAN$102,000[8].

7. CONTROVERSY

Although there are benefits to teaching and employing ethical hacking techniques, there are problems that lead some to question the practice. It is feared that schools may be teaching dangerous skills to students that are unable to make correct decisions on how to use them.

Marcus J. Ranum, a computer security professional has openly objected to the term ethical hacker, saying "There's no such thing as an 'ethical hacker' - that's like saying 'ethical rapist' - it's a contradiction in terms" [9]. A significant part of the controversy surrounding ethical hacking arises from the older definition of hacker and its association with the idea of a computer criminal. However, some organizations do not seem to mind the association and have had a significant increase in careers where CEH and other ethical hacking certifications are preferred or required.

7.1. ETHICAL ISSUES

One of the concerns about teaching ethical hacking is that the wrong people may be taught very dangerous skills. Hacking skills were traditionally acquired by many hours of practice or intense tutoring from another hacker. University programs and commercial training classes are now offering a new way for aspiring hackers to learn how to penetrate systems. Teaching students how to attack systems without providing ethical training may be teaching criminals and terrorists how to pursue their illegal activities. Some individuals have compared teaching ethical hacking to undergraduate students to handing them a loaded gun [10].

7.2. LEGAL LIABILITY

Adding ethical hacking to a curriculum raises a variety of legal issues where schools and faculty members may be held responsible for the actions of their students. The use of many hacking tools outside of an isolated test network may be illegal. By allowing unmonitored hacking sessions, the school or faculty member may be allowing a breach of the law or violation of software licensing agreements. In a case of The United States versus Morris, a judge determined that the Computer Fraud and Misuse Act (18 USC 1030) applies to educational institutions and that an individual is liable for the accidental release of malware. The schools that facilitated the creation of malware would be liable for damages from malware released from their labs.

7.3. FORCING SERVICES AND INFORMATION ON ORGANIZATIONS AND SOCIETY

Sometimes ethical hackers operate without the permission or knowledge of the owners of a system. The rationale given for this is that they are only testing security and do not intend to cause damage or compromise any individual's privacy. However, ethical hackers may be able to uncover information about Web sites and applications that the owners of these sites and applications do not want uncovered. The situation is compared to finding a note on your refrigerator informing you that "I was testing the security of back doors in the neighborhood and found yours unlocked. I just looked around. I didn't take anything. You should fix your lock." This situation is what leads to the necessity for a proper test plan and strict guidelines for following it .

8. REFERENCE

1. Twincling Society Ethical Hacking Seminar. 2006. Retrieved March 27, 2009.
2. Krutz, Ronald L. and Vines, Russell Dean. The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking. Published by John Wiley and Sons, 2007.
3. Palmer, Charles. Ethical Hacking. Published in IBM Systems Journal: End-to-End Security, Volume 40, Issue 3, 2001.
4. Tiller, James S. The ethical hack: a framework for business value penetration testing. Published by CRC Press, 2005.
5. Beaver, Kevin and McClure, Stuart. Hacking For Dummies. Published by For Dummies, 2006.
6. Certified Ethical Hacking Seminar. 2006. Retrieved March 27, 2009.
7. Certified Ethical Hacking EC-Council. 2009. Retrieved March 27, 2009.
8. Certified Ethical Hacking EC-Council. 2009. Retrieved March 27, 2009.
9. Ethical Hacking Jobs. 2009. Retrieved March 27, 2009.
10. D'Ottavi, Alberto. Interview: Father of the Firewall. 2003. Retrieved March 27, 2009.
11. Livermore, Jeffery. What Are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?. Published in Proceedings of the 11th Colloquium for Information Systems Security Education, 2007.

9. SEE ALSO

1. Operating Systems Security
2. Bluetooth Security
3. AJAX Security
4. The Mitnick attack
5. Internet Worm Defenses
6. Information security awareness
7. Social engineering
8. Malware

10. EXTERNAL LINKS

- Ethical Hacking - Introduction to Ethical Hacking
- Web Application Hacking - Basics of Web Application Ethical Hacking
- Vulnerability Assessment Executive Summary WebPower Application
- Ethical hacking: The other side of the fence
- EC-Council CEH
- Whitehats Society
- SATAN Homepage

11. CONCLUSION

In conclusion, ethical hacking is not a criminal activity and should not be considered as such. While it is true that malicious hacking is a computer crime and criminal activity, ethical hacking is never a crime. Ethical hacking is in line with industry regulation and organizational IT policies. Malicious hacking should be prevented while ethical hacking which promotes research, innovation, and technological breakthroughs should be encouraged and allowed.